Technology Advisory Group Meeting
October 18, 2013 2-3:30 PM

Name	Organization
Adrian Gropper	HealthURL Consulting
Keith Worthley	BIDMC
Pat Rubalcaba	Partners Healthcare
Larry Garber	Atrius Health
Claudia Boldman	EOHHS
Anurag Lal	EOHHS
Darlene Vendittelli	The Dimock Center
Sarah Moore	Tufts Medical Center
Atia Amin	Network Health
Pamela May	Partners Healthcare
Ian Rowe	Guest - Orion Health
KT Tomlins	Guest - Orion Health
Support Staff	
Micky Tripathi	Massachusetts eHealth Collaborative
Mark Belanger	Massachusetts eHealth Collaborative
Jennifer Monahan	Massachusetts eHealth Collaborative

Review of Materials and Discussion

Project Updates

- Mass HIway Phase 1- Transaction and Deployment Update (as of Sept 2013) (Slide 2)
    - Eight organizations moved into production (exchanging patient data) in September, making the total number 24. One organization went live (connected by not exchanging data) totaling 11.
    - An update on the number of transactions was provided. In September there were 110,547 transactions, overall totaling over 1,557,181 transactions, 55 organizations have signed agreements and are in various stages of connectivity.
- Phase 2 Overall Timeline (Slide 3)
    - Most of the Public Health Nodes are now live or in testing. The preliminary approach to the Phase 2 Design is complete, but the Design team is still open to feedback and the go-live for Phase 2 is slated for November 2013- March 2014.

Mass HIway Phase 2- Reactions to the Near Final Design

- Setting the Table for Today's Discussion (Slide 5)
    - Several EHR vendors have decided to become Health Information Service Providers (HISPs). Exchange to exchange trust needs to be addressed soon. For

the purposes of today's discussion the focus will be on the technology behind HISP-HISP connectivity.
    - Establishing HISP –HISP trust
    - Certificate exchange
    - Provider directories across HISPs
    - Transport standards (single HISP versus multiple)
- EHR Vendors Expected to Connect to the HIway via Vendor HISP (Slide 6)
    - A list of ten vendors requesting to connect as a HISP was provided. *Note: Epic should be removed from the list.
- HIway HISP Technical Approach (Slide 7)
    - HIway will support the exchange of Anchor Cert with other HISP's:
        - There are two possible approaches Orion could have taken:
            - Mingle Certificates and cross Certify so that it covers two HISPs. This is complex technically and the worry is if a HISP were to mingle with another HISP to cross Certify, they may have already mingled with another—"all of America on one HISP." –OR-
            - Chosen approach: When you become a HISP you are given a root key (source of all of the Certificates you can issue), Orion will take the Certificate from the root key and confirm that it has been signed; the HISP has already provided a Certificate to match against.
    - Anchor Certs are "discoverable" via Web Service.
        - There will be a place to hold the Certs, and mechanisms to provide the HIway Cert back to the HISP.
    - HIway/HISP providers will be on-boarded into "White List."
        - Orion plans to put the HISPs on a Whitelist for validation that the organization is trustworthy; Orion will exchange Certificates with the vendor before adding them to the White List. Participants can also be removed from the white list.
    - HIway Provider Directory listing will be available to HISP via Web Service and Bulk Download.
        - Expose a web service so the user can discover where the message is coming from.
        - Certain HISPs will have a large number of participants in Massachusetts so Bulk Upload/Download functionality is available.
    - S/MIME.
        - The Direct protocol calls for both S/MIME or XDR and XDM. HISP-HISP connectivity requires the use of S/MIME, Orion has chosen to support

S/MIME only to simplify the issues around having both XDR and S/MIME; if you have a mismatch between sender and receiver, you will need to find a way to convert, unencrypt and re-encrypt the message.

- Question: Are there standards for these web services?
  - Answer: No, there are no standards for validation. Orion will be developing criteria so that organizations can check if the Certificate received was derived from the HIway.
- Question: Is this a standard that vendors are typically using?
  - Answer: It is a manual process now, and will be new for vendors. We will verify the identity of the sender/receiver and encrypt the message, but will not encrypt the email header. If the S/MIME signature is not verified using source key, there will be a manual process in place.
- Question: Who can access the White list? Will it be exposed to the provider so they can make sure the organization is trustworthy?
  - Answer: Take eCW for example, if there is an eCW user from Connecticut that is not in the provider directory/White List and they somehow got a direct address of a provider from a Mass HIway HISP, it would not get delivered. There is an eligibility process that the Mass HIway requires of all of its users- they do not self-enter information. The challenge is that that statewide HIE has certain requirements in statute, which is part of the driver for the creation of the Whitelist.
- Question: Why would we not expose the White list to the provider through the EHR or portal? It is not clear how this system will be sustainable; there are too many alternatives for Direct messaging that would bypass the HIway.
  - Answer: It is really about business process constraints, particularly with the Massachusetts opt-in requirements which dictate the White list approach. The use of the Anchor Certs and a White List would allow a message to be automatically flagged as coming from an untrusted source. A provider could create a personal White list that could be maintained at the provider level with the providers trusted partners.

- HIway HISP Solution Overview (Slide 8)
  - The diagram illustrates how the three sources of connectivity (Webmail, LAND or XDR) will interact with the HIway. First, a HISP will exchange its Anchor Certs with the HIway and the Cert is stored in a Hardware Security Module (HSM). Provider White Lists are created and validated. When messages are exchanged and decrypted using Anchor Certs they become “discoverable.”

- Question: What if there is a breach? Will the organization be removed from the Whitelist?
  - Answer: It would be a serious inconvenience because they would need to reissue the Cert. It is expensive and a major disruption that would affect multiple HISP's.
- Question: Will there be an alert for when the Cert is no longer valid? Or expires?
  - Answer: Yes, it does include a lot of those Key management capabilities.
- Question: Is this an alternative to using the Certification authority in one way? Why would we not use existing Certificate authorities?
  - Answer: This is a way to store the trust anchors, to allow a service to be exposed, allowing the gateway/HIDP to query to see if the Cert and signature they receive in a message leads back to the Trust Anchor that has been stored. Storing the Cert says that bilateral agreements are in place- added to the White List of credentialed members of our trust community.

- Implementation Approach (Slide 9)
  - The steps involved in the implementation process were explained. The plan is to start with vendors which have a large stake in getting their providers on- eCW and Surescripts. There is a lot of value in one party staking out this approach and letting others react.
  - Question: Will the HISPs we are interacting with have a parallel agreement, policies and procedures to protect Certs?
    - Answer: Yes, as part of the Vendor Integrator Agreement each party will agree to take care of each other's Certs. The issue is that we don't want those little Certs floating around, if someone were to hack in, they are getting their hands on a lot of information-downstream certificates. They will not have the key, just the Cert which is retrieved from the key.

Next Steps

- Reactions to be taken into account by Phase 2 design team, many of whom were on the call today.
- Meeting notes synthesized and provided back to Advisory Group for final comments.
- Presentation materials and notes to be posted to EOHHS website.

- Next Advisory Group Meeting – December, 20 2:00-3:30
    - Conference call (866) 951-1151 x. 8234356
- HIT Council – Nov 12, 3:30-5:00 One Ashburton Place, 21st Floor

- **HIT Council meeting schedule, presentations, and minutes may be found at http://www.mass.gov/eohhs/gov/commissions-and-initiatives/masshiway/hit-council-meetings.html**